Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

RECHENZENTRUM

Newsletter des Rechenzentrums

Ausgabe Dezember 2022

1. Inhalt

Wir wünschen allseits ein frohes Weihnachtsfest und alles Gute für 2023!

1. Sichere Weihnachten – der CIO-Weihnachtsgruß

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

Hacker machen leider keine Ferien. Vielmehr werden im IT-Bereich gerade die Feiertage dazu genutzt, Schwachstellen auszunutzen und kriminelle Handlungen zu begehen. Aus diesem Grund möchten wir Ihnen jetzt kurz vor Weihnachten ein paar Tipps geben, wie Sie Ihren Beitrag leisten können, damit wir alle ruhige und erholsame Feiertage verbringen können.

1) Sicher einkaufen

Haben Sie noch nicht alle Weihnachtsgeschenke gekauft? Dann muss es jetzt schnell gehen. Zum Glück bieten im Internet viele Anbieter noch garantierte Lieferung vor Heiligabend. Aber Achtung, bei aller Eile sollte auch die Sicherheit eine Rolle spielen. Sie wollen ja Ihre Konto- oder Kreditkartendaten nicht einem Verbrecher übermitteln. Wenn Sie bei einer neuen Plattform bestellen möchten, müssen Sie sich dort erst einen Account anlegen – bitte nehmen Sie hier unbedingt Zugangsdaten, die Sie an keiner anderen Stelle verwenden. Keinesfalls dürfen Sie das gleiche Passwort verwenden, welches Ihrem JMU-Account zugeordnet ist.

2) Neue Endgeräte sicher in Betrieb nehmen

Vielleicht liegt unter dem Weihnachtsbaum ein neues Tablet, ein Smartphone oder ein Notebook? Bevor Sie dieses verwenden, sollten Sie Folgendes beachten: Leider werden Endgeräte oft mit veraltetem Betriebssystem oder ohne Virenschutz ausgeliefert. Angreifern wird es damit möglicherweise leicht gemacht. Bitte nehmen Sie sich die Zeit, als erstes das Betriebssystem und die installierte Software auf den neuesten Stand zu bringen und am besten auch gleich „automatische Updates“ zu aktivieren. Auch ein aktueller (und richtig konfigurierter) Virenschutz von Anfang an ist wichtig.

3) Misstrauisch sein gegenüber unerwarteten E-Mails

Verspricht Ihnen eine Mail plötzlich die Chance auf ein Vermögen? Oder sollen Sie unbedingt den Anhang einer Mail öffnen? Wenn ein Angebot zu gut klingt, um wahr zu sein, seien Sie bitte vorsichtig. Und bitte denken Sie daran: Sie werden niemals in den Weihnachtsferien (und auch sonst nicht) vom IT-Support des Rechenzentrums die Aufforderung erhalten, Ihr Passwort zur Verifikation auf einer Seite einzugeben, welche Sie durch den Link in einer Mail erreichen (Von Ihrer Bank erhalten Sie so eine Mail übrigens auch nicht!). Seien Sie bitte auch in der Weihnachtszeit kritisch und vorsichtig, um nicht auf Phishing in einer Mail hereinzufallen.

4) Vorsicht auf Reisen

Nutzen Sie die Urlaubstage für eine Reise? Diese können Sie besser genießen, wenn sie sich auch in IT-Belangen sicher verhalten. Seien Sie dazu vorsichtig mit kostenlosen WLAN-Angeboten, da hier Ihre Daten unverschlüsselt übertragen werden können, deaktivieren Sie automatische Bluetooth-Verbindungen und geben Sie Ihre Account-Informationen (Benutzername und Passwort) nur auf Endgeräten ein, denen Sie zu 100% vertrauen (also nicht auf dem frei zugänglichen Internet-Terminals am Urlaubsort).

Ihr Rechenzentrum wünscht Ihnen frohe Feiertage und einen guten Rutsch in das Jahr 2023.

Matthias Funken
CIO und Leiter des Rechenzentrums

2. IT-Notfallkarte

Die in den letzten Wochen stark zunehmenden Angriffsversuche auf IT-Infrastrukturen rücken auch die Nutzerinnen und Nutzer wieder in den Fokus. Jeder kann seinen Beitrag leisten, dass es nicht zum Äußersten kommt und am Ende der gesamte IT-Betrieb eine länger andauernde Notabschaltung erfahren muss.

Um Ihnen bei möglichen Sicherheitsvorfällen ein Gerüst mit an die Hand zu geben, hat das Rechenzentrum der JMU eine „Notfallkarte“ erstellt.

Abbildung 1: IT-Sicherheitsvorfall auf einen Blick

Diese Karte zeigt alle relevanten Informationen, die für eine möglichst zeitnahe Reaktion beim Beobachten ungewöhnlicher IT-Vorfälle zu beachten sind.

Entsprechende PDF-Versionen können Sie hier herunterladen und am besten direkt an der von Ihnen genutzten PC-Hardware anbringen:

Link für PDF-Vorlagen zur IT-Notfallkarte

Auf dieser Webseite finden sich auch Plakate, die ausgedruckt gerne in allen Gebäuden der JMU aufgehängt werden dürfen.

3. Einstellungen für sichere Zoom-Meetings

Immer wieder ist bundesweit von Vorfällen zu hören, bei denen Zoom-Meetings „gekapert“ werden und Störenfriede sich in der jeweiligen Veranstaltung breit machen. Aus aktuellem Anlass möchten wir nochmals auf die verschiedenen Möglichkeiten hinweisen, Zoom-Meetings so abzusichern, dass es nicht zu etwaigen Störungen einer Online-Veranstaltung kommen kann.

Denn noch immer werden trotz Präsenzbetrieb an der JMU jeden Tag ca. 900 auch größere Meetings abgehalten. Dabei ist immer dann besondere Achtsamkeit gefragt, wenn Sie als Meetingveranstalter eine Nachricht von Zoom erhalten: „**Your Zoom meeting is at risk“ („**Ihr Zoom-Meeting ist gefährdet“)

Diese Meldung von Zoom wird immer dann automatisiert versendet, wenn ein Meeting offen im Internet beworben wird. „Offen“ heißt in diesem Fall, dass es keine oder nur wenige Schutzmaßnahmen für eine Teilnahme bei dem anberaumten Online-Termin gibt. Dabei können folgende Einstellungen des Meetings helfen, potentielle Störaktionen zu verhindern:

- **Webinar-/Meeting-Link**
  Verbreiten Sie den Webinar- bzw. Meeting-Beitrittslink nicht öffentlich (bspw. auf Plattformen wie Facebook oder Twitter). Nutzen Sie zur Verlinkung auf Ihre Veranstaltung besser die Seiten der Universität.
- **Registrierungsfunktion**
  Meetings und Webinare können per Registrierungsfunktion sicherer gemacht werden, da sich TeilnehmerInnen zunächst authentifizieren müssen, bevor der Beitrittslink zugesandt wird.
- **Warteraum**
  Aktivieren Sie den Warteraum, um zu verhindern, dass während der Veranstaltung Personen unerlaubt das Meeting betreten.
- **Sperren**
  Sperren Sie das Meeting, wenn alle angemeldeten Teilnehmer bereits teilnehmen. So verhindern Sie, dass weitere Personen an dem Meeting teilnehmen können.
- **Chatfunktion deaktivieren**
  Bei großen Veranstaltungen empfiehlt es sich ggf., die Chatfunktion vollständig zu deaktivieren, oder nur Direktnachrichten an den Host zu ermöglichen. So kann unter anderem Hasskommentaren vorgebeugt werden.
- **Stummschaltung**
  Stellen Sie die Teilnehmer auf Stumm und deaktivieren Sie die Möglichkeit, die Stummschaltung aufzuheben (Unterbindung von Störungen/ Hasskommentaren)
- **Bildschirmfreigabe**
  Deaktivieren Sie die Möglichkeit, dass Teilnehmende den Bildschirm freigeben können. (Unterbindung von Störungen/ Hasskommentaren)

- **Virtueller Hintergrund**
  Deaktivieren Sie die Möglichkeit, dass Teilnehmende einen virtuellen Hintergrund einsetzen können. Beachten Sie: Die Möglichkeit des virtuellen Hintergrundes dient primär zum Schutz der Privatsphäre der Teilnehmenden. Bei hoch kontroversen Themen kann die Deaktivierung auch zur Unterbindung von Hasskommentaren dienen.
- **Q&A-Funktion (für Webinare)**
  In Webinaren eignet sich die Q&A-Option für Fragen

Weitere Umfangreiche Einstellungstipps erhalten Sie auf den Webseiten zu Zoom:

Anleitungen zur Zoom-Nutzung

4. Windows 10 Version 21H1: Support endet

Eine weitere Windows 10 Version geht in den Ruhestand. Der Support von Windows 10 „21H1“ endet im Dezember 2022, siehe dazu auch die Meldung von Microsoft:

Link zu Informationen Windows 10 Version 21H1.

Alle IT-Betreuer wurden über betroffene Rechner bereits durch die wöchentlich versandten Sperrlisten informiert. Bitte führen Sie auf diesen Rechnern ein Feature Upgrade durch, spätestens im Januar werden die betroffenen Geräte in unserem Verzeichnisdienst gesperrt. Damit wäre eine weitere Nutzung ausgeschlossen.

5. Phishing Mails – Important News! (Deutsche Version darunter)

We are currently exposed to a strong flood of phishing emails. The treacherous thing is that the short e-mails sometimes look like official messages from the data center to you. In truth, however, possible entries on your part are misused, for example to send SPAM mails with the then hacked accounts or to do worse.

Therefore, please pay close attention to whether the e-mails are really messages from the university or so-called phishing e-mails. In cooperation with an external security company, we have also put various short videos on the WueCampus e-learning platform, which explain in an understandable way what everyone can do for their own IT security and that of the university.

Please watch the videos found at these links:

Short videos by the company SoSafe to raise user awareness Part 1
Short videos by the company SoSafe to raise user awareness Part 2

DEUTSCHE VERSION:

Wichtige Nachricht für unsere Nutzer:

Wir sehen uns aktuell einer starken Flut von Phishing-Mails ausgesetzt. Das Tückische ist dabei, dass die kurzen Mails für Sie teilweise wie offizielle Nachrichten aus dem Rechenzentrum aussehen.

In Wahrheit werden aber mögliche Eingaben Ihrerseits missbraucht, um zum Beispiel mit den dann gehackten Accounts von Ihnen SPAM-Mails zu versenden oder Schlimmeres anzurichten.

Abbildung 2: Gemeinsam gegen Phishing-Mails! (Abbildung Fa. SoSafe)

Bitte achten Sie daher genau darauf, ob es sich bei den Mails wirklich um Nachrichten aus der Universität handelt oder eben um sogenannte Phishing-Mails.

In Kooperation mit einer externen Sicherheitsfirma haben wir auf der eLearning-Plattform WueCampus auch verschiedene Kurzvideos abgelegt, die in verständlicher Weise aufklären, was jeder für die eigene IT-Sicherheit und die der Universität machen kann. Bitte schauen Sie sich die Videos an, die unter diesem Link zu finden sind:

Link zur eLearning-Plattform WueCampus mit den Kurzvideos

6. Neues Onlinebuchungssystem für den Geräteverleih

Was ist der Geräteverleih?

Für den medientechnischen Einsatz innerhalb der Hochschule steht Ihnen im Rechenzentrum schon seit 2008 eine breite Palette an Geräten inkl. entsprechendem Zubehör kostenlos zur Verfügung.

Das Angebot umfasst eine große Anzahl an medientechnischem Equipment. Sie finden Aufnahmegeräte, Beamer, Leinwände, Digitalkameras, Audioanlagen mit Mikrofon und Mischpult, Laptop, Videobars für hybride Lehrszenarien bis hin zu LED-Großdisplays und Videoproduktionssets.

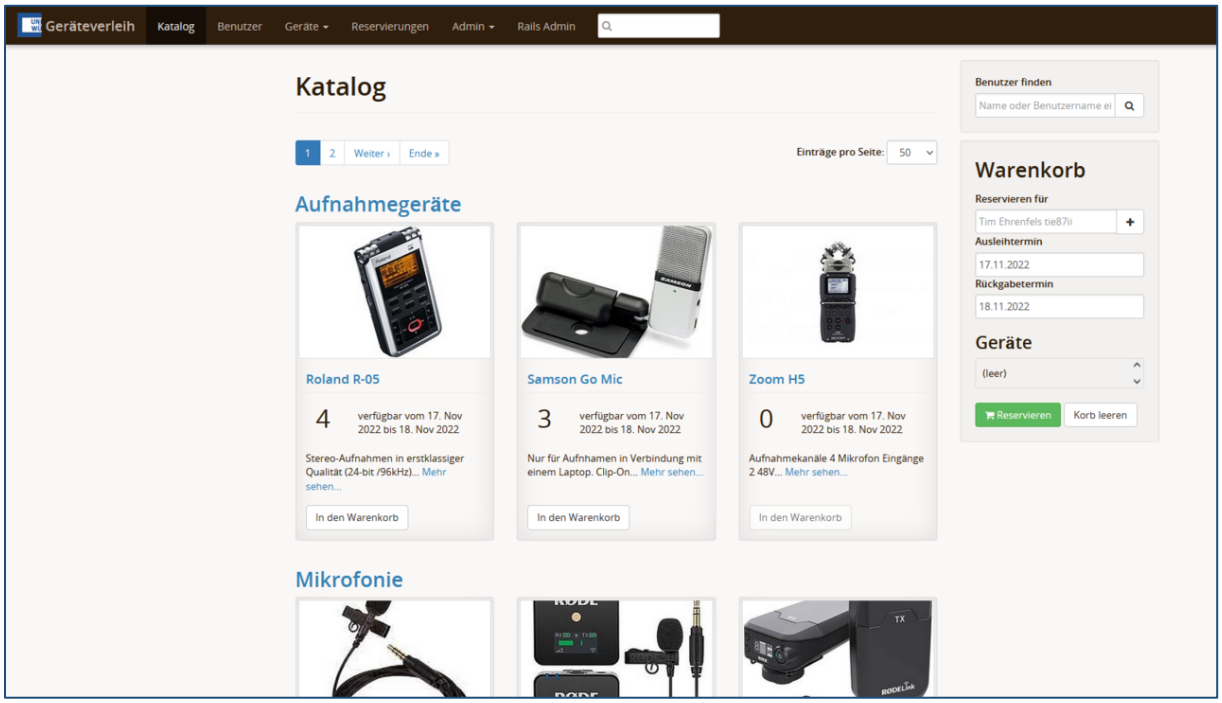

Abbildung 3: Screenshot des neue Geräteverleih-Systems

Wichtig: Die Leihe ist nur möglich zu *dienstlichen Lehr-, Lern- und Forschungszwecken*! Weitere Informationen finden Sie hier:

Informationen zum Geräteverleih

Das neue Geräteverleihsystem ist nur aus dem Uni-Netz heraus erreichbar, von extern ist eine VPN-Verbindung (weitere Infos dazu im Link) notwendig.

Aktuelle Öffnungszeiten: Montag und Dienstag von 9.00 bis 16.00 Uhr. Mittwoch, Donnerstag und Freitag ist der Geräteverleih geschlossen.

Bei Fragen zum Geräteverleih wenden Sie sich gerne an: geraeteverleih@uni-wuerzburg.de

Noch ein zwei allgemeine Hinweise

Bitte bleiben Sie beim Ausleihen fair und ermöglichen Sie auch anderen Einrichtungen der Uni, das entsprechende Equipment nutzen zu können. Das betrifft vor allem die maximale Verleihdauer von 5 Arbeitstagen. In Ausnahmefällen und nur nach vorheriger Anfrage kann dieser Zeitraum auch verlängert werden. Bitte haben Sie aber Verständnis, dass der Verleih kein Ersatz für eigene Hardwarebeschaffungen sein kann.

Achten Sie auch auf Vollständigkeit und pfleglichen Umgang, damit noch viele nachfolgende NutzerInnen von den Geräten profitieren können.

7. Einheitliches Mailadressensystem für Mitarbeitende

Historisch gesehen gibt es zahlreiche Varianten in der Darstellung von eMailadressen an der JMU. Leider haben sich zuletzt immer häufiger gravierende Nachteile der vormals genutzten Adressierung gezeigt.

Probleme ergeben sich dabei…

- in der automatisierten Pflege der Adressen im Verzeichnisdienst
- in der Konfiguration von mailnahen Systemen (z.B. Load Balancer, VPN),
- in der Zertifikatsverwaltung von Servern und Diensten oder
- in der Betreuung der NutzerInnen im IT-Support.
- durch funktionale Einschränkungen bei der Nutzung von Cloud Services (z.B. von Microsoft).

Aus diesem Grund wurde im Oktober im IT-Beratungsgremium beschlossen, den Mailadressen an der JMU eine einheitliche Struktur zu geben.

E-Mailadressen werden seit Mitte November nach folgendem Schema eingerichtet:

- Alle Mitarbeitenden:
  Vorname.Nachname@uni-wuerzburg.de
- Alle Studierenden:
  Vorname.Nachname@stud-mail.uni-wuerzburg.de
- Ausnahmen:
  - Bei langen Namen, insbesondere Doppelnamen und Namensergänzungen, wird bei Bedarf gekürzt.
  - Bei Namensgleichheit mit einer schon bestehenden Adresse wird eine (möglichst geringfügige) Modifikation vorgenommen.
  - Bisher genutzten Adressen werden als Alias erhalten bleiben.

Auch für die vielfach genutzten, sogenannten Funktionsaccounts (z.B. bei Sekretariaten) ergeben sich Änderungen.

Alle neuen Regelungen können zusammengefasst auf dieser Webseite nachgelesen werden:

Hinweise zum Aufbau von eMail-Adressen an der JMU

8. Wir suchen Dich - Studentische Hilfskraft im Posterdruck/Geräteverleih

Das Rechenzentrum bietet ab sofort eine Stelle als studentische Hilfskraft (m/w/d) im Bereich Posterdruck und Geräteverleih an.

Zum Aufgabereich zählen

- der Druck von Postern für den universitätsweiten Posterdruck,
- die Ausgabe und Rücknahme der Geräte des Geräteverleih
- sowie das Zurücksetzen und Aufbereiten der Geräte.

Entsprechendes Engagement, Team- und Terminfähigkeit werden erwartet. Die Arbeitszeit beträgt nach Absprache bis zu 30 Stunden/Monat. Es wird eine langfristige Beschäftigung angestrebt.

Bei Interesse bitten wir um eine Kurzbewerbung mit Lebenslauf per E-Mail an Tim Ehrenfels (Adresse: tim.ehrenfels@uni-wuerzburg.de).

9. Neue Stabsstelle „IT-Security“

IT-Security spielt eine weiterhin zunehmende Bedeutung für die JMU, was sich in vielen bereits ergriffenen Maßnahmen widerspiegelt:

- Verabschiedung der Leitlinie für Informationssicherheit und Datenschutz durch die Universitätsleitung (Link zur Webseite mit dem Dokument)
- Ernennung des Informationssicherheitsbeauftragten (ISB, Prof. Samuel Kounev),
- Verabschiedung des Sicherheitskonzeptes der JMU (Link zur Webseite mit dem Dokument)
- Beschaffung einer neuen Firewall
- Phishing-Sensibilisierungsmaßnahmen für unsere AnwenderInnen
- Einbeziehung von Dienstleistern zur Bekämpfung von Cyber-Angriffen

Dies sind nur einige Beispiele für die kürzlich ergriffenen organisatorischen und technischen Maßnahmen. Das Rechenzentrum hat seine Organisation diesem Bedeutungszuwachs angepasst und die neue Stabsstelle „IT-Security“ im RZ unter der Leitung von Helmut Celina gegründet. Die aktualisierte Version des organisatorischen Aufbaus des Rechenzentrums finden Sie unter folgendem Weblink zum Organigramm.

10. Neuer Rahmenvertrag Medientechnik und Apple

Die Ansprüche aus aktuellen Lehr- und Lernszenarien wachsen stetig. Nicht zuletzt sind aus der Pandemie-Situation Bedarfe entstanden, die durch den noch aktuellen Rahmenvertrag für medientechnische Hardware nicht zu bedienen waren.

In den letzten 12 Monaten gab es in Bayern auch deswegen eine Neuausschreibung des Rahmenvertrages „Medientechnik“ mit zahlreichen neuen Produktklassen. Mit nunmehr 27 teilnehmenden Hochschulen im Freistaat ist er der größte Vertrag seit Beginn der Ausschreibungen in diesem Beschaffungsbereich.

Neu sind neben Videobars für hybride Lehrszenarien u.a. auch interaktive Whiteboards. Der neue Vertrag startet Anfang Januar. Wir werden im Anschluss auch den Webshop mit den neuen Produkten ergänzen.

Auch für Produkte des Herstellers Apple wurde in den vergangenen Monaten ein neuer Rahmenvertrag ausgearbeitet. Alle weiteren Informationen dazu finden Sie unter folgendem Link:

Informationen zum neuen Apple Rahmenvertrag

11. Keine Nutzung von MS Sharepoint und OneDrive für personenbezogene Daten

Das an der JMU häufig genutzte „Teams“, aber auch andere Microsoft-Dienste nutzen zum Speichern von Dateien bei Gebrauch die Onlinedienste „Onedrive“ und „Sharepoint“. Die Speicherung von personenbezogenen Daten in der Cloud ist aber an der Uni Würzburg grundsätzlich nicht zulässig, siehe auch:

Hinweise zur Arbeit mit Microsoft 365

Nutzer können unter Link zum Login für Microsoft Online einsehen, welche Daten (versehentlich oder aus Unkenntnis heraus) unter ihrem Account gespeichert sind und diese dort auch löschen.

12. Öffnungszeiten zum Jahreswechsel

Wie der Rest der Universität auch, hat das Rechenzentrum vom 24.12.2022 bis einschließlich 1.1.2023 geschlossen. Ab Montag, 2.1.2023 ist das Gebäude wieder geöffnet. Der IT-Support ist in der Kalenderwoche 1 per Mail erreichbar:

it-support@uni-wuerzburg.de

Posterdruck und Geräteverleih haben vom 2.1. bis 5.1. noch geschlossen.

Das ganze RZ-Team wünscht Ihnen allen ein frohes Weihnachtsfest und ein gutes Neues Jahr!

Ende des Newsletters „Dezember 2022“